# **Systems** @ INESC-ID

## Técnico Lisboa

The **D**istributed, **P**arallel and **S**ecure **S**ystems Group of INESC-ID

inesc id lisboa 20 YEARS

DEFINING TECHNOLOGY

inesc-id.pt

# surething

# Project Overview

Miguel.Pardal@tecnico.ulisboa.pt

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

inesc id lisboa
20 YEARS
DEFINING TECHNOLOGY

TÉCNICO LISBOA

# Outline

- Research Context
- Goal
- Work Packages
  - Use Cases
- Expected Contributions

# Research Context

- The **scale** and geographic dispersion of the Internet of Things (IoT) will surpass the size of the current day Internet
  - By, at least, **3 orders of magnitude**
- The IoT will be the largest and most widely distributed system ever, with a multitude of connected sensors and actuators
- The current Internet already has some serious, unresolved security issues
  - Adding physical world connections brings even more concerns about **attacks** and their consequences to **people** and **goods**

# Location

- Location Based Services (LBS) provide geographic or topological context
  - To mobile applications
  - To Internet of Things applications
- Usually the location is detected by the device and then trusted by the applications

# Location Estimation Techniques

GPS

Wi-Fi

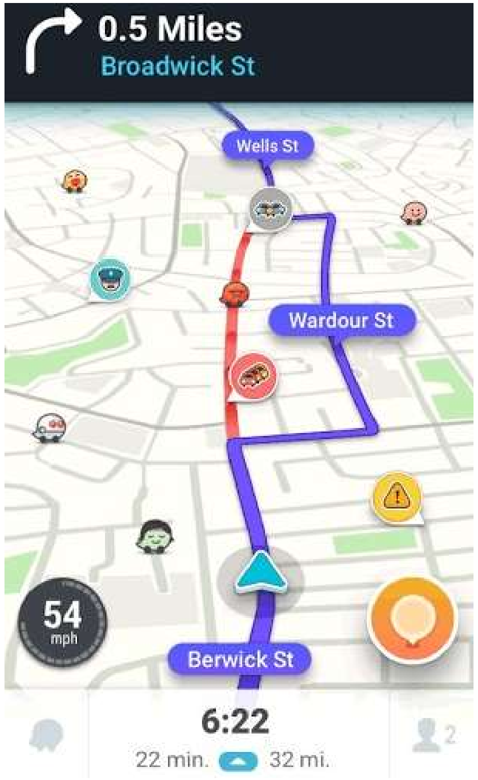
Bluetooth

…

# Location example: Car Navigation

- Insert destination
- Detect geographic location
- Retrieve map for coordinates
- Display map
- Plot path

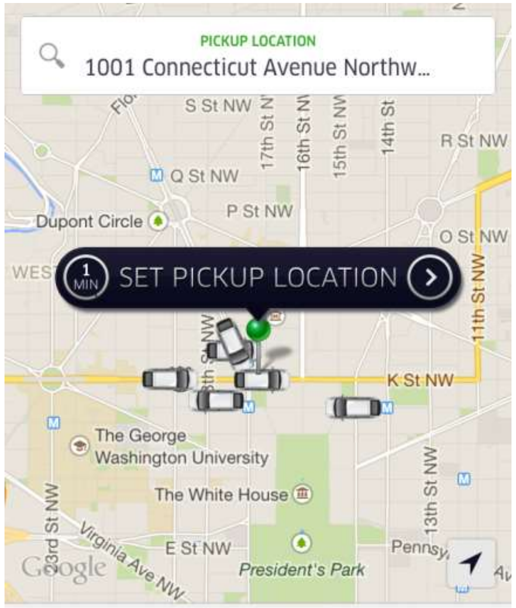
- Committed resources belong to the **user**



# Location reverse example: Hail Cab

- Insert destination
- Detect geographic location
- Insert pickup location
- Hail cab
  - Wait for it

- Committed resources belong to the **cab**



PICKUP LOCATION

1001 Connecticut Avenue Northw...

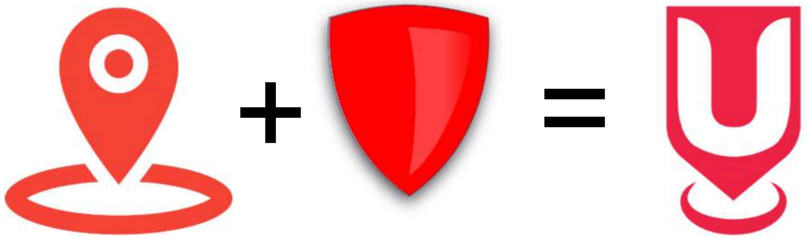
1 MIN SET PICKUP LOCATION

# Location Proofs

- There are instances where we want to be **sure** the **thing** is there
  - Is the thing really at the claimed location?
  - The location of the device must be proved!

- This way, the device location can be a certified attribute
  - That can be used for making security policy decisions

- Analogy: as **identity** needs **authentication**, **location** needs to be **proven**
  - Challenge-response



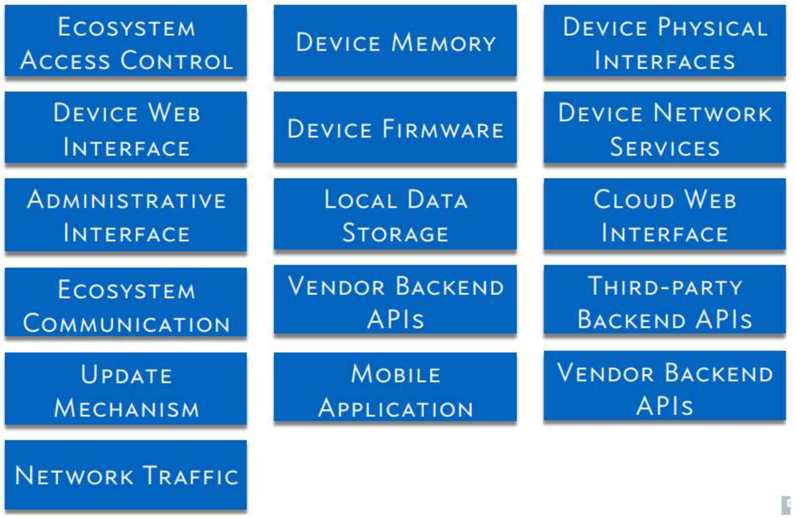
# Challenge-Response for verifying presence at location

- If devices could talk, it would be something like:

- “Hey, X, if you are really at location Y as you claim, then…
  - tell me signal strengths from all nearby devices!
  - tell me the level of ambient noise for the past 3 seconds!
  - tell me …

# Idea

- Turn the heterogeneity of the IoT – complex systems, with large attack surface – into a security advantage
  - Observe unique features of each location and capture its specific traits
  - Compare against pattern or witness



| | | |
|---|---|---|
| Ecosystem Access Control | Device Memory | Device Physical Interfaces |
| Device Web Interface | Device Firmware | Device Network Services |
| Administrative Interface | Local Data Storage | Cloud Web Interface |
| Ecosystem Communication | Vendor Backend APIs | Third-party Backend APIs |
| Update Mechanism | Mobile Application | Vendor Backend APIs |
| Network Traffic | | |

# Goal

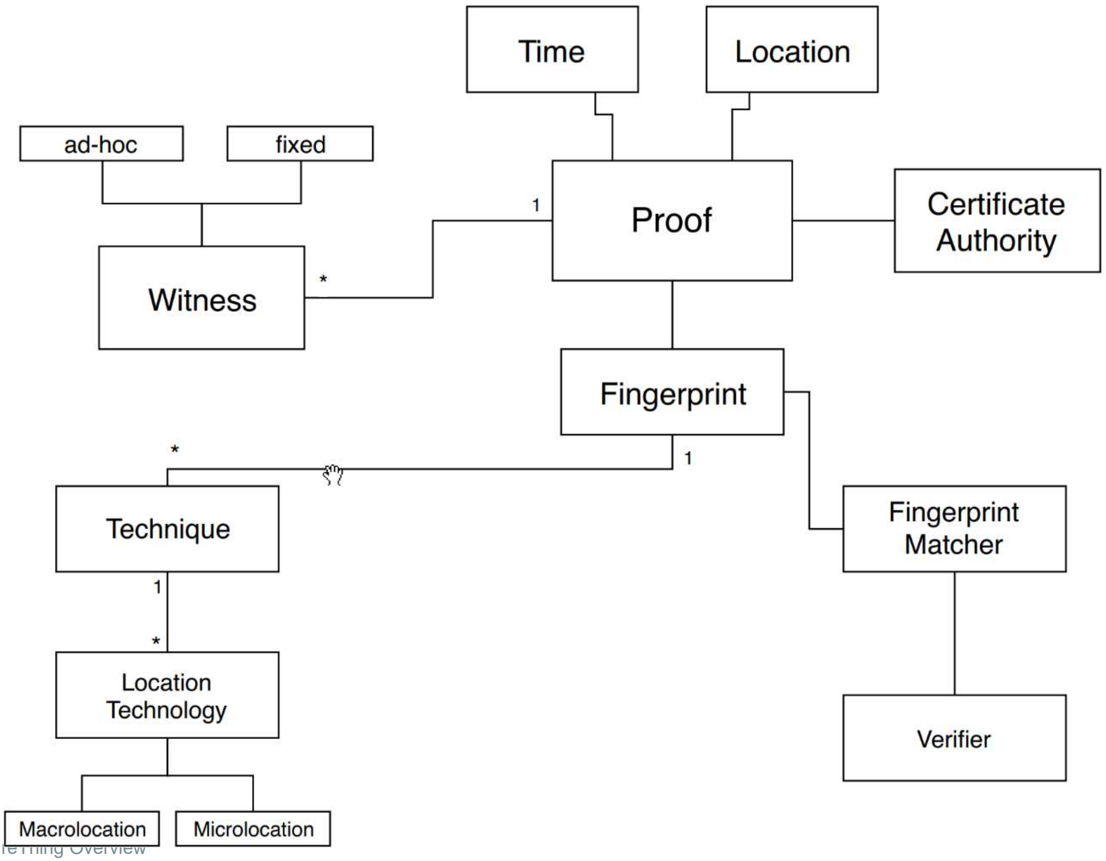
- The project **goal** of SureThing is to provide a flexible **framework** to support creating and validating location of devices using **diverse** challenge-response techniques

- Create and validate location proofs
  - Devices can certify their location or ask for location certificates from other devices
- Proofs can be used to make security decisions
  - E.g. trustworthy attributes for policy decision in ABAC solution
- For Internet of Things applications:
  - Mobile devices allow human interaction
  - Limited devices
  - Smart Spaces

# Location certificates

- The location certificates issued using the SureThing framework contain:
  - location data, obtained and verified using one or more techniques
  - locality-sensitive network measurements, using WiFi and Bluetooth fingerprinting, and ambience sensing

# Conceptual model



# Witnesses and beacons

- Beyond the uniqueness of locations, the security model of SureThing is reinforced with **witness** models
  - Someone can say what they saw
  - Ad-hoc (circumstantial) witness
- **Beacons**
  - Add more information to allow more unique fingerprints
  - Transmit sequences generated from secret seed
    - Usually time-bound
  - Ask of prover (and witnesses) to capture the signal
  - The verified can then check if the transmission was correctly received
  - And make the assumption that the device was there

# Use Cases

- This project will validate its contributions using two use cases:
- **Smart Tourism**
  - Key economic sector in Portugal
  - Build an application providing tourists with awards for each visit to a predefined set of locations, making use of reliable fast location proofs
  - Use existing infrastructure
- **Smart Taxes / Inspections**
  - Use dedicated infrastructure and agents
  - Intended to be collusion-resistant
  - Stronger proofs: combine the locations proofs with digital notaries
    - with time-stamping
    - long-term archival

# Work Packages (WP)

- WP1: API Interfaces and Data Schemas
  - To be completed
- WP2: Witness models
  - Working prototypes for ad-hoc and trusted witnesses
  - Missing: integration with identity providers
- WP3: Location Proof Techniques
  - Wi-Fi, Bluetooth
  - To explore: Cellular, GPS, ambient sensing

# Work Packages (cont.)

- WP4: Smart Tourism Use Case
  - Working prototype for city trek
- WP5: Distributed Proof Ledgers
  - To be developed
- WP6: Smart Taxes Use Case
  - Working prototype for vehicle inspection

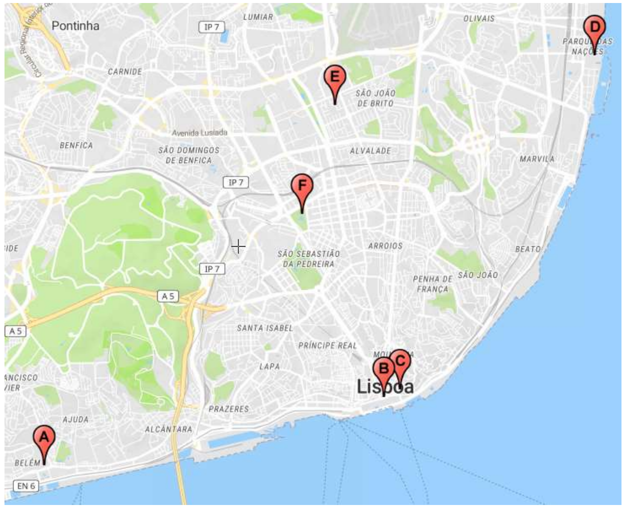
# Support WPs

- WP7: Impact and Outreach
- WP8: Project Management

# What are we doing now

- Wi-Fi scavenging for proofs
- Composite proofs in smart spaces
- Privacy protections
- (Framework libraries)

# Wi-Fi scavenging for proofs



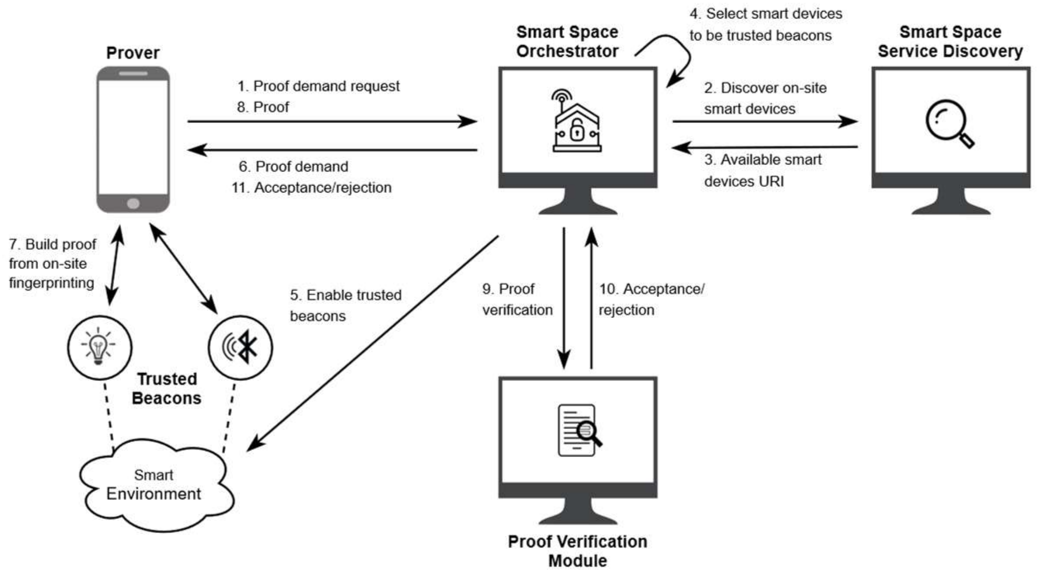
- Wi-Fi traces scavenged provide new opportunities
  - Compiled these traces into a dataset
  - Of various points of interest in the city of Lisbon

- Extend the scavenging method of CROSS (Smart Tourism)
  - To provide time-bound location proofs

- Use the diversity of Wi-Fi networks observed in the dataset
  - **Stable networks** (trigger) to determine **location**
  - **Volatile networks** (hotspots) to determine **time** window

# Composite proofs in smart spaces

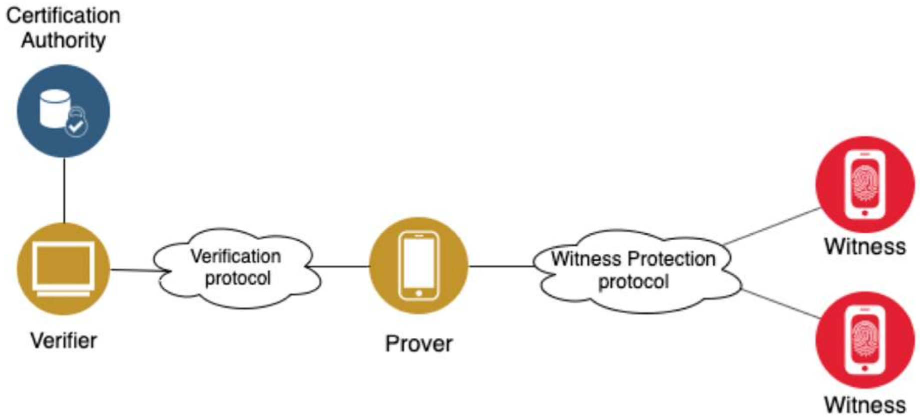
- Leverage instrumented smart devices as trusted beacons
  - Use a smart space management framework to discover, configure and control them
- Use case: hospital cleaning verification (robots or humans)


Prover
Smart Space Orchestrator
Smart Space Service Discovery
4. Select smart devices to be trusted beacons
1. Proof demand request
8. Proof
6. Proof demand
11. Acceptance/rejection
2. Discover on-site smart devices
3. Available smart devices URI
7. Build proof from on-site fingerprinting
5. Enable trusted beacons
9. Proof verification
10. Acceptance/ rejection
Trusted Beacons
Smart Environment
Proof Verification Module

# Privacy protections

- **Witness Protection Protocol** protects the location of the Witnesses
  - This protocol uses Clustering Geo-Indistinguishability mechanism
  - Differential privacy techniques

- **Verification Protocol** protects the identity of the Prover
  - Zero-Knowledge Proofs



# SureThing framework

- **Why do we need a framework?**
- Interoperability
  - Proof formats
  - Proof interpreters
- Extensibility
  - Allow for the novel techniques developed in this project or by the research community to be integrated as they appear
- Diversity
  - Allow the combination of different techniques to provide stronger proofs
- Flexibility - developers can choose between:
  - Faster location proofs vs more elaborate and reliable proofs
  - Single or multiple techniques
  - Witnesses from deployed infrastructure or found at the moment (ad-hoc)

# Expected Contributions

- Novel research is needed to enable secure location proofs for the IoT
- Location you can **trust** and **verify**
  - The widespread use of SureThing location proofs will significantly improve the security decisions of policies for the IoT.
  - This will lead to more secure and trustable services in the near future

# Summary

- We expect location proofs to be used in the Internet of Things as much as digital certificates are part of every web site that we visit today

- Open framework will make state-of-the-art techniques available and will be extensible to incorporate new techniques as they become available

- Tested in useful applications
  - Provide value
  - Comply with security practices in place today
  - Produce proofs suited to the use case requirements

# Team

- Current
  - Rui Claro (PhD Candidate)
  - João Tiago (MSc Candidate)
  - João Costa (MSc Candidate)

- Soon
  - 2 Post-Docs
    - Avijit and Leonardo, if all goes well

surething

inesc id lisboa 20 YEARS

DEFINING TECHNOLOGY

# Thank you!

This work is supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with project reference PTDC/CCI-COM/31440/2017.